In the Claims:

Please amend Claims 58, 59, 64, 65, 69, 71, 113, 115, 117, 119-122 and 148; cancel Claims 60-63, 66, 67, 70, 72-76, 120, 121, 123-127, 133-135, 147, and 149-156; and add new Claims 157-170, all as shown below. Applicant reserves the right to prosecute any originally presented or canceled claims in a continuing or future application.

58. (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

a central policy manager for managing and distributing a security policy; and

an application guard located at a client, said application guard including a customized local policy particular to that client, for managing access by a user of the client to ~~a transaction related with an~~ software application components at the client, as specified by the security policy.

59. (Currently Amended) A system for managing and enforcing complex security requirements to protect computer systems against unauthorized access in a distributed computer network comprising;

a policy manager located on a server for managing and distributing a policy to a client; and

an application guard located on the client, acting to grant or deny access by users of the client to various software application components of the client, as specified by the ~~security~~ policy.

60-63. (Canceled).

64. (Currently Amended) The system of claim 59 wherein the client contains a program stored in non-volatile memory for granting or denying access to various software application components ~~or resources~~ of the client, as specified by the policy distributed from the server.

65. (Currently Amended) The system of claim 59 wherein the server includes a non-volatile memory storing the policy manager that specifies the security requirements for software applications and database objects;

said policy contains security rules that describe at least one constraint that constrains

which software applications a particular user can access and

which database objects within an software application a user can access.

66-67. (Canceled).

68. (Original) The system of claim 59 wherein the policy is organized into groups and hierarchies.

69. (Currently Amended) The system of claim 59 wherein the policy includes access rules, which include:

a grant rule that grants a privilege to a ~~subject~~ first user on ~~an object~~ a software application component under a first constraint; and

a deny rule that denies a privilege to a ~~subject~~ second user on ~~an object~~ the software application component under a second constraint.

70. (Canceled).

71. (Currently Amended) [[The]] A system for managing and enforcing complex security requirements to protect computer systems against unauthorized access in a distributed computer network comprising ~~of claim 59 the policy manager further comprises~~:

a policy manager located on a server for managing and distributing a policy to a client; and

an application guard located on the client, acting to grant or deny access to various software application components of the client, as specified by the policy;

an audit log data file to record authorization requests;

an optimized policy data file;

an enterprise policy data file;

an administrative policy data file; and

a local administrative policy data file.

72-76. (Canceled).

77. (Withdrawn) A system comprising a computer having a security policy that includes at least one or more components having at least:

an object,

a subject,

a privilege, and

a condition.

78. (Withdrawn) The system of claim 77 wherein each object can be an application or an operation within an application.

79. (Withdrawn) The system of claim 77 the object is capable of being set to be at least any of:

an application,

a method,

a web page,

a database table

a file, and

one or more menu items in a graphical user interface.

80. (Withdrawn) The system of claim 77 wherein the object can be organized into at least an object hierarchy such that:

if a user is granted a certain privilege on a parent object, then that user is automatically granted the privilege on all the children objects, and

if a user is denied a certain privilege on a parent object, the that user is denied the privilege on all the children objects.

81. (Withdrawn) The system of claim 77 wherein the privilege is capable of being inherited from a parent to a child object.

82. (Withdrawn) The system of claim 77 wherein the subject is capable of being set to be at least any of:

a user and

a role containing one or more users, who can at least

access a protected object, and

have access to at least some information in the system.

83. (Withdrawn) The system of claim 77 wherein the subject is capable of being a user that can be chosen to be either internal or external to a system.

84. (Withdrawn) The system of claim 77 wherein the object comprises a list that is capable of containing one or more users authorized to access the object who can no log on to the object and be authenticated by the object through an external authentication server.

85. (Withdrawn) The system of claim 77 wherein the system is capable of having the subject be a user who at least:

can be maintained separately by one or more components each of which can be an object or directory server; and

can be extracted from said one or more components to synchronize the components thereby maintaining their access account.

86. (Withdrawn) The system of claim 77 wherein components comprise an alias-user who at least inherits all privileges of a user under certain conditions, thereby facilitating authorization management by providing fine granularity of control on propagation of a privilege.

87. (Withdrawn) The system of claim 86 wherein the system is capable of having the alias-user be created to perform a job function while the user is absent, and inheritance of the privilege takes effect only when the user is absent.

88. (Withdrawn) The system of claim 77 wherein a user of the object is capable of being defined to be local to the object.

89. (Withdrawn) The system of claim 77 wherein a user can be at least a global user mapped to a set of local users having at least one local user per object.

90. (Withdrawn) The system of claim 77 wherein the privilege defines at least one kind of access that is allowed to the object and includes at least one right to perform a particular action on the object.

91. (Withdrawn) The system of claim 77 wherein the privilege is capable of including at least
a right to execute an application,
a right to download a web page,
a right to query a database table, or
a right to view a menu item.

92. (Withdrawn) The system of claim 77 wherein the component is capable of being assigned to be a wild card that is capable of being used at least as a privilege, object, or subject.

93. (Withdrawn) The system of claim 77 further comprising an access request that includes at least:
a privilege,
an object , and
a subject;
wherein the access request is used by at least a subject to request authorization of at least a privilege on at least an object.

94. (Withdrawn) The system of claim 93 wherein the access request at least:

matches a grant rule if the privilege, object, and subject match those in the rule, and the constraint in the rule is met; and

matches a deny rule if the privilege, object, and subject match those in the rule, and the constraint in the rule is not met.

95. (Withdrawn) The system of claim 77 wherein the access request is at least:

denied if

there is a deny rule matching the request, or

there are no access rules matching the request; and

granted if there are no deny rules matching the request and there is a grant rule matching the request.

96. (Withdrawn) The system of claim 77 wherein certain conditions comprise constraints and the system has at least facilities for defining constraints as expressions formed from operators including at least NOT, AND, and OR.

97. (Withdrawn) The system of claim 77 wherein conditions at least:

are constraints on when the object or the subject can be accessed,

specify requirements on when the access rule is applicable, and

contain options that can be set to be dependent on properties on the object or the subject.

98. (Withdrawn) The system of claim 77 wherein the system further comprises facilities for expressing constraints at least:

1) relational operations on integers,

2) relational operations on strings; and

3) set operations.

99. (Withdrawn) The system of claim 77 wherein the system further comprises facilities that allow the user to define conditions.

100. (Withdrawn) The system of claim 77 wherein the system includes an Application Programming Interface (API) for invoking user-supplied code to evaluate user-defined functions.

101. (Withdrawn) A system comprising a computer having a security policy that includes at least one or more components having at least a set of privileges that includes at least one privilege that is capable of at least:

being granted to a user explicitly; and

being granted to a role which is granted to the user.

102. (Withdrawn) The system of claim 101 wherein:

the role is a named group of privileges containing at least one privilege that are granted to at least one user or to at least one other role; and

the at least one user granted the role is a member of the role.

103. (Withdrawn) The system of claim 101 wherein the members of a role automatically inherit all the privileges granted or denied to the role.

104. (Withdrawn) The system of claim 101 wherein roles are organized into a role hierarchy, where parent roles are granted to children roles such that:

if a parent role is granted a privilege, then the children roles are automatically granted the privilege; and

if a parent role is denied a privilege, then the children roles are automatically denied the privilege.

105. (Withdrawn) The system of claim 101 wherein roles of an object may be defined as being local to that object.

106. (Withdrawn) The system of claim 101 wherein the role is at least a global role mapped to at least a set of local roles, having at least one role per object.

107. (Withdrawn) The system of claim 101 wherein the system further comprises more than one role, two of which have memberships that are mutually exclusive with respect to one another.

108. (Withdrawn) A security system comprising a policy manager located on a computer system that includes at least:

a management console or station;
a database management system;
an audit facility; and
a distributor.

109. (Withdrawn) The system of claim 108 wherein the management station comprises a Graphical User Interface (GUI) for users to create and customize rules by system users.

110. (Withdrawn) The system of claim 108 wherein the management station supports concurrent rule development by multiple users.

111. (Withdrawn) The system of claim 108 wherein the management station includes an application guard to allow only authorized administrators to operate the management station based on at least a local administrative policy which provides a set of policy rules specifying which users are authorized to access the management station.

112. (Canceled).

113. (Currently Amended) A security system comprising:

an application guard located within non-volatile memory of a client that is designed to reside along with each protected software application component on that client and supports transactional access control by allowing [[an]] the software application to detect an authorization service and to make authorization requests at each user interaction, data request, and business level transaction by a user or application of the client.

114. (Original) The security system of claim 113 further comprising a distributor capable of distributing the application guard to clients located throughout an enterprise.

115. (Currently Amended) The system of claim 113 wherein the application guard is coupled to the software application through an application programming interface (API) or authorization library that allows the software application components to request authorization services as needed through an application guard interface.

116. (Original) The system of claim 113 further comprising

an authorization engine that processes an authorization request;

a checker that parses local client policy and stores the parsed local client policy in Random Access Memory (RAM); and

an evaluator that evaluates the authorization request with the parsed local client policy in RAM to determine whether the authorization request should be granted or denied.

117. (Currently Amended) The system of claim [[113]] 116 wherein the authorization engine comprises plug-ins that at least allow for additional capabilities to process and evaluate authorization request based on customized code.

118. (Canceled).

119. (Currently Amended) The system of claim 113 wherein the system is capable of implementing at least:

the application guard locally to the software application; and

the application guard as a remote authorization service through a remote procedure call to another server.

120-121. (Canceled).

122. (Currently Amended) A method for maintaining security in a distributed computing environment comprising:

managing a central security policy via a policy manager; and

managing access by a user of the client via an application guard at a client to a transaction related with ~~an~~ a software application component on that client, as specified by the security policy.

123-127. (Canceled).

128. (Withdrawn) The method of distributing at least one security policy rule comprising:

passing the policy rule through at least

a DataBase (DB) layer and

an Open DataBase Connectivity (ODBC) layer; and

storing the policy rule as an enterprise policy.

129. (Withdrawn) The method of claim 128, wherein:

the (DB) layer formats the policy rules into standard database storage tables, and

the (ODBC) provides a common interface to various vendor-specific databases.

130. (Withdrawn) The method of claim 128, wherein the distribution occurs through the (ODBC) layer and a communication interface.

131. (Withdrawn) The method of claim 128 further comprising passing the enterprise policy to a distributor.

132. (Withdrawn) The method of claim 128 further comprising determining via an optimizer program within the distributor which application guard needs to receive the policy rules.

133-135. (Canceled).

136. (Withdrawn) A method of managing policy under management services in a management station comprising:

an authorized administrator logging into a policy manager;

the authorized administrator choosing either administrative mode to manage administrative policy or enterprise mode to manage administrative policy;

presenting the administrator with menu options including

navigate tree,

analyze policy,

edit policy,

distribute policy,

view audit log to allow the administrator to view and track authorization requests that have occurred at an application guard connected to a system, and

exit.

137. (Withdrawn) The method of claim 136 wherein the menu option navigate tree provides a set of edit options for an administrator that include to

add,

delete, and

modify features; and

wherein the administrator is presented with a choice of features on a server and on a client.

138. (Withdrawn) The method of claim 136 wherein the features to which the administrator can apply the edit policy option include

global users,
global roles,
directories,
local roles,
local users,
applications,
application guards, and
declarations.

139. (Withdrawn) The method of claim 136 wherein the menu option analyze policy allows an authorized user to analyze and view rules and policies within the enterprise policy.

140. (Withdrawn) The method of claim 136 wherein the administrator is presented with options
to search rules, and
to query policy.

141. (Withdrawn) The method of claim 140 wherein if search results is selected, the administrator is presented with options of searching grant rules and all the deny rules pertaining to a particular user.

142. (Withdrawn) The method of claim 140 wherein if query policy is selected, a search can be made on who is granted or denied what privilege on which objects under what conditions.

143. (Withdrawn) The method of claim 140 wherein the menu option edit policy presents an authorized user with the option to add, delete, and modify enterprise policy features.

144. (Withdrawn) The method of claim 143 wherein the features that may be edited include
a rule set,
access,

a privilege,

an object,

a user,

a role, and

an attribute.

145. (Withdrawn) The method of claim 136 wherein the menu option distribute policy includes distributing the new features of a newly entered or modified enterprise policy to appropriate application guards.

146. (Withdrawn) The method of claim 136 wherein upon selecting the distribute policy option

a distributor optimizes enterprise policy;

a differ program computes a difference between a newly optimized policy and a formerly optimized policy;

the newly optimized policy is then published as optimized policy in DBMS;

only the changed portions of the newly optimized policy are committed to an appropriate application guard;

the application guard receives the changed portions of the newly optimized policy;

the application guard merges the received changed portions into local client policy; and

the local client policy is activated to work with the application guard.

147. (Canceled).

148. (Currently Amended) ~~The method of claim 147 wherein evaluating the authorization request includes an evaluator searching deny rules in a local policy, and~~ A method of granting client access authorization comprising:

using an application guard that includes at least

requesting access to a software securable component associated with an application protected by the application guard, wherein the application guard constructs and issues and authorization request, and

evaluating the authorization request via the application guard according to its local client policy to determine whether to allow or deny the authorization request; and

wherein evaluating the authorization request includes an evaluator searching deny rules in the local client policy, and if the evaluator finds a deny rule, then an evaluation is performed on any constraints on the deny rule, if the evaluation finds a presently valid constraint on the deny rule, then access is denied, and if the evaluation finds that all constraints on the deny rule are not presently valid, then a search for a grant rule is performed, and if no deny rules are found, then a search for a grant rule is performed;

wherein after a search for a grant rule if no grant rule is found that would allow access for the user, then access is denied, and if a grant rule is found, then an evaluation is performed on any constraints in the grant rule wherein if the evaluated constraint is presently valid, then access is allowed, and if the evaluated constraint is not presently valid, then access is denied; and, an audit records the authorization request in an audit log;

wherein if there is an error is the authorization request, or if the request is not valid, then access is denied; if the authorization request is valid, then a determination is made whether access should be granted, and if the evaluated authorization request does not deny access, then access is allowed, and if the evaluated authorization request denies access, then access is denied.

149-156. (Canceled).

157. (New) A system for maintaining security in a distributed computing environment, comprising:

a policy manager for managing a security policy; and

an application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, for managing access to securable components as specified by the

security policy, said securable components being selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

158. (New) The system of claim 157, wherein said policy manager further comprises a distributor for distributing the security policy to a client.

159. (New) The system of claim 157, wherein said system is scalable by further comprising a plurality of clients, said policy manager further managing and distributing a customized local policy to each client, and at least one additional application guard located on each client for managing access toll the securable components as specified by each customized local policy.

160. (New) The system of claim 159, wherein said application guard includes an application guard interface coupled to an application for requesting access to the securable components, and at least one authorization engine for evaluating requests from the application guard interface as specified by a customized local policy based on the security policy.

161. (New) The system of claim 160, wherein said application guard interface is located on a client, and said at least one authorization engine and said customized local policy are located on a client server.

162. (New) A system for controlling user access in a distributed computing environment, comprising:

a global policy specifying access privileges of the user to securable components;

a policy manager located on a server for managing and distributing a local client policy based on the global policy to a client, and

an application guard located on the client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, for managing access to the securable components as specified by the local client policy, said securable components being selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

163. (New) The system of claim 162 further comprising at least one additional client, said policy manager further managing and distributing a customized local policy based on the global policy to each additional client, and at least one additional application guard located on each additional client for managing access to the securable components as specified by the customized local policy.

164. (New) The system of claim 162, wherein said system is scalable by further comprising a plurality of clients, said policy manager further managing and distributing a customized local policy to each client, and at least one additional application guard located on each client for managing access to the securable components as specified by each customized local policy.

165. (New) The system of claim 162, wherein said application guard includes an application guard interface coupled to an application for requesting access to the securable components, and at least one authorization engine for evaluating requests from the application guard interface as specified by the local client policy.

166. (New) A system for managing security in a distributed computing environment, comprising:

a policy manager specifying access privileges to securable components selected from the group consisting of at least one application; a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application;

an application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, for managing access to securable components; and

a processor coupled to said system, said processor executing said policy manager to manage and distribute a customized local policy based on a global policy to a client,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

167. (New) A method for maintaining security in a distributed computing environment, comprising the steps of:

managing a policy using a policy manager by specifying access privileges of a user to securable components selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application; and

distributing the policy to a client having an application guard, said application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, whereby the application guard manages access to the securable components as specified by the policy,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with

each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

168. (New) A method as claimed in claim 167 for maintaining security on a client in a distributed computing environment, further comprising the steps of:

constructing and issuing an authorization request for a user to access to securable components located on the client using the application guard;

evaluating the authorization request using the application guard to determine if the authorization request is valid or invalid; and

allowing access to the user via the application guard if the evaluated authorization request was valid, and denying access to the user via the application guard if the authorization request was invalid.

169. (New) A computer-readable medium comprising program instructions for maintaining security in a distributed computing environment by performing the steps of:

managing a policy using a policy manager by specifying access privileges of a user to securable components selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application;

distributing the policy using the policy manager to a client having an application guard, said application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, whereby the application guard manages access to the securable components as specified by the policy; and

executing said policy manager with a processor to manage and distribute the policy,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

170. (New) A system for maintaining security in a distributed computing environment, comprising:

means for managing a policy using a policy manager by specifying access privileges of user to securable components selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application;

means for distributing the policy using the policy manager to a client having an application guard, said application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, whereby the application guard manages access to the securable components as specified by the policy; and

means for executing; the policy manager to manage and distribute the policy,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.